

REMARKS/ARGUMENTS

This amendment is in response to the Office Action dated February 3, 2004. Claims 1-13 are pending. Claims 1 and 7 have been amended. Claims 1-13 remain pending in the present application.

Amended Claims

Applicants have amended independent claims 1 and 7 to clarify the present invention. In particular, claim 1 was amended to recite “capturing biometric information of the user by the computer system,” “encrypting the biometric information using a secure server’s public key and signing the biometric information with a private key of the computer system,” “sending the encrypted and signed information from the computer to the secure server in the network,” and “accepting and verifying credentials associated with the signed and encrypted information from the secure server utilizing the public key from the secure server.” Support for these amendments is found throughout the Specification, for example at page 9, line 9 to page 10, line 3. Accordingly, no new matter has been presented.

Claim 7 was amended to recite that the secure server is “coupled to the computer system” and that it “includes a database that stores credential information associated with biometric information,” and that “if the secure server authenticates the user via the biometric information, the secure server sends the associated credential information to the computer system such that the user can securely operate the computer system.” Support for this amendment is found throughout the Specification, for example at page 9, lines 1-3, and at page 9, line 21 to page 10, line 7. Accordingly, no new matter has been presented.

35 U.S.C. §103 Rejections

The Examiner rejected claims 1-13 under 35 U.S.C. § 103(a) as being unpatentable over Musgrave et al. (U.S. Patent No. 6,202,151) in view of Gilchrist (U.S. Patent No. 6,167,517). In so doing, the Examiner stated:

In regards to claim 1, 6-8, and 13, Musgrave discloses a biometric certificate which may be generated by concatenating transaction data, a public key, and the set of data, including the biometric data (Musgrave: column 4, lines 53-55). This meets the limitation of "capturing biometric information of a user; encrypting using server public key." The authenticating certificate is then hashed to generate a hashed value. The hashed value is then sent to a registration authority having a biometric certificate generated where the hashed value is then signed; that is, encrypted, using the private key of the user to generate a digital signature incorporating the biometric data. The digital signature is then appended to the transaction data (Musgrave: Column 5, lines 15-35). This meets the limitation of "signing the biometric information with a client private key." After receiving the electronic transaction from the network a receiver decrypts the transaction using it's private key, de-hashes the decrypted transaction and extracts the biometric certificate. The receiver then sends the biometric certificate to the biometric certificate management system (BCMS) for authentication (Musgrave: column 5, lines 36-47). This meets the limitation of "sending the encrypted and signed data to a secure server in the network; accepting and verifying credentials associated with the signed and encrypted data from the server utilizing the public key from the central server." However, Musgrave does not disclose "installing the credentials into the computer if the credentials are verified."

Gilchrist discloses the biometric template is stored locally on the client system and discloses adding new templates to the system (Gilchrist: column 1, lines 51-65). This meets the limitation of "installing the credentials into the computer if the credentials are verified."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of authentication using a biometric authenticating certificate as disclosed by Musgrave with the method of storing the biometric template locally as disclosed by Gilchrist in order to guard against a malicious user who substitutes another template to gain unauthorized access to the host system (Gilchrist: abstract).

Applicants respectfully traverse.

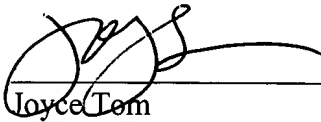
In view of the foregoing, it is submitted that the claims 1-30 are allowable over the cited references and are in condition for allowance. Applicant respectfully requests reconsideration of the rejections and objections to the claims, as now presented.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

May 3, 2004
Date



Joyce Tom

Attorney for Applicant(s)
Reg. No. 48,681
(650) 493-4540